

MacPherson Kwok Chen & Heid LLP

1762 Technology Drive, Suite 226
San Jose, CA 95110
Tel. (408) 392-9250
Fax (408) 392-9262

2402 Michelson Drive, Suite 210
Irvine, CA 92612
Tel. (949) 752-7040
Fax (949) 752-7049

Email: mailbox@macpherson-kwok.com

RECEIVED
CENTRAL FAX CENTER

FEB 21 2006

February 21, 2006

Via Facsimile to (571) 273-8300

Mail Stop APPEAL BRIEF - PATENTS

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Re: Applicants: Lane Lee, et al.
Assignee: DPHI Acquisitions, Inc.
Title: Mastering Process and System for Secure Content
Application No.: 09/939,960 Filing Date: August 27, 2001
Examiner: Firmin Backer Group Art Unit: 3261
Docket No.: M-12043 US Confirmation No.: 6648

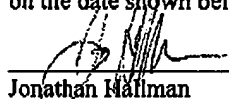
Dear Sir:

Transmitted herewith are the following documents in the above-identified application:

- (1) This Transmittal Letter (1 page); and
- (2) Appellants' Opening Brief (11 pages).
- (3) Petition for Extension of Time

☒ The fee has been calculated as shown below:

- ☒ Fee for Filing Brief in Support of an Appeal (SMALL ENTITY) \$250.00
- ☒ Petition for Extension of Time (2 months): If an extension of time is required for timely filing of the enclosed document(s) after all papers filed with this transmittal have been considered, an extension of time is hereby requested. \$225.00
- ☒ Please charge our Deposit Account No. 50-2257 in the amount of \$ \$475.00
- ☒ Also, charge any additional fees required and credit any overpayment to our Deposit Account No. 50-2257

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Jonathan Hallman February 21, 2006
Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicant
Reg. No. 42,622

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Lane W. Lee

Application No. 09/939,960

Filing Date: 08/27/2001

For: Mastering Process and System For
Secure Content

Examiner: Firmin Backer

Art Unit: 3621

Attorney Docket No.: M-12043 US

APPELLANTS' OPENING BRIEF

02/23/2006 CNGUYEN 00000012 502257 09939960

01 FC:2402 250.00 DA

Real Party In Interest

The real party in interest is DPHI Acquisitions, Inc., the present assignee of US Application No. 09/939,960.

Related Appeals and Interferences

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1 – 36 are cancelled.

Claims 37 – 43 are pending and are twice rejected.

The rejection of claims 37 – 43 is appealed.

Status of Amendments

No amendments have been filed since the 2nd non-final rejection.

Real Party In Interest

The real party in interest is DPHI Acquisitions, Inc., the present assignee of US Application No. 09/939,960.

Related Appeals and Interferences

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1 – 36 are cancelled.

Claims 37 – 43 are pending and are twice rejected.

The rejection of claims 37 – 43 is appealed.

Status of Amendments

No amendments have been filed since the final rejection.

Summary of Claimed Subject Matter

The present invention relates to digital rights management (DRM). In conventional DRM systems, the host (such as a PC) is where the DRM processing is conducted. This location is inherently vulnerable to hacking. Thus there is a need for improved DRM systems. However, content users have legitimate expectations as well that should not be violated by an overly-restrictive DRM system. To address this need in the art, Applicants have provided a DRM system in which DRM "intelligence" is incorporated into the storage engine such as a CD-ROM drive, magnetic hard drive, etc. As opposed to conventional DRM systems that reside on the host, an integrated storage engine approach is far less vulnerable to hacking by a host system user – the user has no access to DRM functionality within the storage engine other than through reading and writing of secure content according to rules governed by the storage engine itself. The user knows that digital content may flow to and from the data storage medium but cannot access the "how" within the storage engine that enabled such movement. Moreover, the integration of the DRM system into the storage engine is advantageous in portable applications. Different host systems such as kiosks at a content provider retail outlet or a personal computer may be more readily modified to couple to the portable DRM-system-integrated storage engine.

Regardless of where the DRM functionality is integrated (host or storage engine), an integral part of DRM systems involves the right of the content provider to revoke access privileges of content users. In conventional DRM schemes, the revocation is "all or nothing" in that after authentication of a user, the user's identity is checked for revocation. If the user is indicated as revoked, no file access is granted. In addition to their storage-engine-DRM-implementation described above, Applicants have improved upon this all-or-nothing revocation scheme. In addition to making a global revocation decision at the time of authentication, a revocation decision may be made later on a file-by-file basis. In other words, a user may be revoked as to file A but not as to file B. This improved "granularity" to the revocation process gives greater control and flexibility to the DRM implementation.

Aspects of this DRM-system-integrated storage engine with a granular file-by-file revocation scheme may be seen in Applicants' Figure 6 and the accompanying description on pages 29 and 30. A host seeking access to content (or wishing to write content) on a storage medium 602 controlled by storage engine 604 first provides a certificate 610 to become authenticated. Before being authenticated, the host will be checked for revocation using revocation list 608. As described for example, on page 45 through 78 of the specification, the storage engine may read security metadata from the storage medium to provide "functionality to the CKDRM and TPDRM methods, including lock/unlock, CKDRM play, [and] CKDRM copy permissions." (page 46, lines 5-6). Thus, a user may wish access to a certain file but be denied (revoked) as to this file because, for example, it remains locked, or the user does not have play permission, etc.

Argument

Claim 37 is directed to a content access method incorporating the storage-engine and granular revocation features discussed in the summary section. Specifically, claim 37 includes the acts of "receiving at a storage engine a certificate from the host device, the certificate containing a digital signature; authenticating the digital signature; [and] receiving at the storage engine a file request from the authenticated host device, the file request being directed to a file stored on a storage medium accessible to the storage engine." In response to this file request, the storage engine performs the acts of "reading security metadata associated with the file from the storage medium, the security metadata containing at least one rule governing access to the file; within the storage engine, applying the at least one rule to the file request from the host device; and if the application of the at least one rule provides a failing result, denying the file request."

The Nordman reference (2002/0174073) stands in sharp contrast. Rather than have a granular, file-by-file revocation scheme as discussed with regard to claim 37, the Nordman reference discloses the usual "all or nothing" revocation scheme. In particular, as seen in his Figure 1, Nordman is directed to the protection of privacy for a cell phone/wireless device 110. Through configuration of "profile operators" 115, the cell phone user may develop several privacy profiles depending upon the scenario. A number of examples are described starting at paragraph 198. For example, a shopping scenario is described in paragraph 200, a meeting scenario in paragraphs 202 -203, etc. But note the glaring deficiency in each of these scenarios with regard to the method recited in claim 37. The "host" in each instance does not seek a file from the handset and then get denied. Instead, upon authentication, the host may have access to any file the user has authorized access to in that particular scenario. There is no granularity whatsoever, just the conventional "all or nothing" approach with regard to any particular authenticated host. For example, in the "meeting scenario" of paragraphs 202-203, a user decides what information to provide such as "personal information, software including games, etc., documents, and

Grounds of Rejection to Be Reviewed on Appeal

- 1) Whether, under 35 U.S.C. § 102(a), claims 37 – 20 are anticipated by U.S. Patent Publication No. 2002/0174073 to Nordman, et al.

so forth.” (paragraph 203). If another in this meeting scenario is authenticated, that authenticated user then has access to this information. Nordman has not a shred of suggestion or teaching for attaching rules to the files in the meeting scenario. In other words, if another is authenticated, that authenticated other has rights to whatever has been authorized in this scenario. As such, this “revocation” is no different than any other conventional DRM revocation scheme: if upon authentication, a host is not revoked, that host has access to whatever files the authentication is directed to.

Moreover, the lack of a file-by-file revocation scheme is not the only flaw in the Nordman reference. The Nordman privacy scheme is “host-based” in that it requires a profile operator (element 115) to manage the user’s profile information (paragraph 47). As such, there is no data-storage-engine-based act of “reading security metadata associated with the file from the storage medium” by the user device 110 in Nordman. Instead, a host (the profile operator) determines whether another can access a user’s profile information in Nordman. As discussed above, host-based DRM schemes are inherently less secure than Applicants’ storage-engine-based DRM implementation. Accordingly, claim 37 and its dependent claims 38 – 41 are patentable over the cited prior art.

Claim 42 is also patentable over Nordman for analogous reasons in that claim 42 is directed to a storage engine that includes a “file request response means for responding to file requests from the host device, each file request identifying a particular file, the file request response means being responsive to file requests only if the authentication means authenticates the digital signature, the file request response means being configured to read security metadata associated with the file from a storage medium, the security metadata containing at least one rule governing access to the file; the file request response means being configured to apply the at least one rule to the file request from the host device; the file request response means being configured to deny the file request if the application of the at least one rule provides a failing result.” Such a file request means enables the granular file-by-file revocation discussed previously. In addition, this file request means is part of the storage engine and reads for

Claims Appendix

37. An access method, comprising:

receiving at a storage engine a certificate from the host device, the certificate containing a digital signature;

authenticating the digital signature;

receiving at the storage engine a file request from the authenticated host device, the file request being directed to a file stored on a storage medium accessible to the storage engine;

within the storage engine, reading security metadata associated with the file from the storage medium, the security metadata containing at least one rule governing access to the file;

within the storage engine, applying the at least one rule to the file request from the host device; and

if the application of the at least one rule provides a failing result, denying the file request.

38. (previously presented) The method of claim 37, wherein the at least one rule comprises a plurality of rules.

39. The method of claim 37, wherein the storage medium is an optical disk.

40. The method of claim 37, wherein the application of the at least one rule act comprises checking play privileges for the host device.

41. The method of claim 37, further comprising: if the application of the at least one rule provides a successful result, granting the file request.

42. A storage engine, comprising:

authentication means for authenticating a digital signature contained in a certificate from a host device, and

file request response means for responding to file requests from the host device, each file request identifying a particular file, the file request response means being responsive to file requests only if the authentication means authenticates the digital signature, the file request response means being configured to read security metadata associated with the file from a storage medium, the security metadata containing at least one rule governing access to the file; the file request response means being configured to apply the at least one rule to the file request from the host device; the file request response means being configured to deny the file request if the application of the at least one rule provides a failing result.

43. The storage engine of claim 42, wherein the storage medium is an optical disk.

Evidence Appendix

No evidence was submitted under Rules 130, 131, or 132.

Related Proceedings Appendix

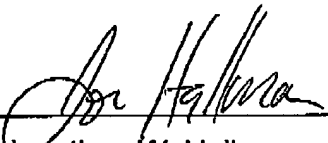
There are no related proceedings.

itself the security metadata (that being a feature of Applicants' "storage-engine-based" DRM implementation). Therefore, claim 42 and its dependent claim 43 are allowable over the cited prior art.

Accordingly, in light of the foregoing arguments, Applicants respectfully request the Honorable Board of Appeals to reverse the decision of the Examiner with respect to claims 37 through 43.

Respectfully submitted,

Date: Feb. 21, 2006

By: 
Jonathan W. Hallman
Reg. No. 42,622